No. 2016-1480

United States Court of Appeals for the Federal Circuit

VIRNETX INC.,

Appellant,

v.

APPLE INC.,

Appellee.

Appeal from the United States Patent and Trademark Office, Patent Trial and Appeal Board, in Reexamination Control No. 95/001,949

BRIEF OF APPELLEE APPLE INC.

Jeffrey P. Kushan
SIDLEY AUSTIN LLP
1501 K Street, NW
Washington, DC 20005
(202) 736-8000

John C. O'Quinn
Nathan S. Mammen
KIRKLAND & ELLIS LLP
655 15th Street, NW
Washington, DC 20005
(202) 879-5000

Counsel for Appellee Apple Inc.

May 26, 2016

U.S. PATENT NO. 8,051,181 B2, CLAIMS 1 AND 2 (APPX 115)
(emphasis added)

1. A non-transitory machine-readable medium comprising instructions for a method of communicating with a first device associated with *a secure name* and *an unsecured name*, the method comprising:

receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desired [sic] to securely communicate with the first device; and

sending a message over a *secure communication link* from the first device to the second device.

2. A method of using a first device to communicate with a second device having *a secure name*, the method comprising:

from the first device, sending a message to a secure name service, the message requesting a network address associated with the secure name of the second device;

at the first device, receiving a message containing the network address associated with the secure name of the second device; and

from the first device, sending a message to the network address associated with the secure name of the second device using a *secure communication link*.

CERTIFICATE OF INTEREST

Counsel for Appellee Apple Inc. certifies the following:

1. The full name of every party represented by us is:
Apple Inc.

2. The name of any real party in interest represented by us, and not identified in response to Question 3, is: N/A

3. All parent corporations and any publicly held companies that own 10 percent or more of the stock of the party represented by us are: Apple Inc. has no parent corporation. No publicly held corporation owns 10% or more of Apple Inc.'s stock.

4. The names of all law firms and the partners or associates that appeared for the party now represented by us in the agency or are expected to appear in this Court are:

Kirkland & Ellis LLP: John C. O'Quinn, Robert A. Appleby, Nathan S. Mammen, Akshay S. Deoras

Sidley Austin LLP: Jeffrey P. Kushan, Joseph R. Guerra, Joseph Micallef, Scott M. Border, Anna M. Weinberg, Raquel C. Rodriguez, Thomas A. Broughan III, Samuel A. Dillon, Ryan C. Morris

May 26, 2016

/s/ John C. O'Quinn
Counsel for Apple Inc.

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Cases

Statutes

STATEMENT OF RELATED CASES

The patent at issue in this appeal, U.S. Patent No. 8,051,181 ("the '181 patent"), was also the subject of *VirnetX Inc. v. Apple Inc.*, No. 6:11-cv-00563, in the United States District Court for the Eastern District of Texas. This action was consolidated with another VirnetX infringement action against Apple, E.D. Texas No. 6:12-cv-00855, which remains pending. Together, these cases additionally involved related U.S. Patent Nos. 6,502,135, 7,490,151, 7,418,504, 7,921,211, and 8,504,697. The Court has not heard any appeals involving the '181 patent.

In *VirnetX, Inc. v. Cisco Systems, Inc.*, 767 F.3d 1308 (Fed. Cir. 2014), the Court affirmed-in-part, reversed-in-part, vacated-in-part, and remanded for further proceedings a final judgment from the U.S. District Court for the Eastern District of Texas involving four of the related patents, U.S. Patent Nos. 6,502,135, 7,490,151, 7,418,504, and 7,921,211. The remanded case (No. 6:10-cv-00417), which remains pending in the district court, was also consolidated for trial with E.D. Texas No. 6:12-cv-00855. Apple is the only remaining defendant, and the case was restyled as *VirnetX Inc. v. Apple Inc.* The case was tried from January 25, 2016 to February 3, 2016 and did not involve the '181

patent. Prior to the appeal, the district court severed VirnetX's request for an ongoing royalty into a separate action (No. 06:13-cv-00211) and entered an order for an ongoing royalty. Following its decision in *Cisco*, this Court vacated the district court's order. *VirnetX Inc. v. Apple Inc.*, No. 14-1395 (Fed. Cir.).

Several other cases involving related patents are pending in this Court and the Patent Trial and Appeal Board ("the Board"). Pending in this Court are the following five appeals from final decisions of the Board involving patents related to the '181 patent:

Federal Circuit Docket No.	Patent Trial and Appeal Board Case No.	Patent No.
15-1934	IPR2014-00237	8,504,697
15-1935	IPR2014-00238	8,504,697
16-1211	IPR2014-00403	7,987,274
16-1213	IPR2014-00404	7,987,274
16-1279	IPR2014-00482	7,188,180
16-1281	IPR2014-00481	7,188,180

Pending before the Board are the following proceedings against related VirnetX patents: IPR2015-00810 and IPR2015-00811 (U.S. Patent No. 8,868,705); IPR2015-00812 (U.S. Patent No. 8,850,009); IPR2015-00866 (U.S. Patent No. 8,485,341); IPR2015-00868 (U.S. Patent No. 8,516,131); IPR2015-00870 and IPR2015-00871 (U.S. Patent

No. 8,560,705); IPR2015-01009 and IPR2015-01010 (U.S. Patent No. 8,843,643); IPR2015-01046 and IPR2016-00062 (U.S. Patent No. 6,502,135); IPR2016-01047, IPR2016-00063, and IPR2016-00167 (U.S. Patent No. 7,490,151); IPR2016-00331 and IPR2016-00332 (U.S. Patent No. 8,504,969); IPR2016-00693 (U.S. Patent No. 7,418,504); IPR 2016-00957 (U.S. Patent No. 7,921,211).

PRELIMINARY STATEMENT

VirnetX's U.S. Patent No. 8,051,181 is one of a large family of patents that purport to disclose an approach for communicating securely over a network such as the Internet. But secure network communications was a crowded field, and the approach claimed by the '181 patent was hardly groundbreaking, let alone novel. Indeed, the Patent and Trademark Office ordered reexamination of the '181 patent after finding substantial new questions of patentability existed for all of its claims, identifying *eleven* different grounds involving *nine* different prior art references. The Board ultimately found it unnecessary to address all of the grounds, because its careful inquiry demonstrated that every single claim was anticipated by at least one of three references—and most were anticipated *thrice over*.

On appeal, VirnetX responds to the Board's fact-intensive determinations with scattershot arguments, attempting to re-litigate nearly every issue the Board decided. VirnetX leads with claim construction arguments recycled from a related appeal (No. 15-1934) that a secure communication link *always* requires encryption. But the Board, as it has multiple times before, properly rejected that

construction for the simple reason that the '181 patent does not support it—let alone under the broadest reasonable interpretation standard used in this reexamination proceeding. Regardless, VirnetX has no answer to the Board's finding that the prior art, in fact, uses encryption. VirnetX also disputes the Board's construction of the terms "secure name" and "unsecured name," arguing that those constructions are unreasonably broad and should be limited to specific embodiments in the '181 patent. It does so despite the fact that those terms *appear nowhere* in the '181 patent's specification. The Board properly rejected VirnetX's circular and unsupported reasoning and construed these terms consistent with the broad scope they connote.

In response to the Board's findings that the Beser, Mattaway, and/or Provino references anticipate every claim of the '181 patent (with all three overlapping in anticipating many claims), VirnetX's arguments largely rise and fall with its erroneous claim construction positions. And VirnetX's challenges to the Board's detailed factual findings are legally flawed or substantively meritless. The Board's factual determinations are amply supported by substantial evidence, and this Court should affirm the findings of unpatentability.

STATEMENT OF THE ISSUES

1. Whether the Board properly construed, under the broadest reasonable interpretation, the terms: (a) "secure communication link" as used in the claims as not requiring encryption, (b) a "secure name" as used in the claims as not being limited a name that is resolved by a "secure name service," and (c) an "unsecured name" as used in claim 2 as not being limited to a name that does not require resolution by a "secure name service."

2. Whether substantial evidence supports the Board's findings that claims 1-12, 14, 15, 17-29 are anticipated by Beser under 35 U.S.C. § 102.

3. Whether substantial evidence supports the Board's findings that claims 1, 2, 7-9, 12-17, 19-21, and 24-29 are anticipated by Mattaway under 35 U.S.C. § 102.

4. Whether substantial evidence supports the Board's findings that claims 1-15, 18-23, 28, and 29 are anticipated by Provino under 35 U.S.C. § 102.

STATEMENT OF THE CASE

VirnetX appeals from the final written decision in Reexamination Control No. 95/001,949, holding claims 1-29 unpatentable.

A. The '181 Patent

The '181 patent (U.S. Patent No. 8,051,181), titled "Method for Establishing Secure Communication Link Between Computers of Virtual Private Network," is one of many related patents VirnetX has obtained that purport to disclose technology for "establishing a secure communication link between a first computer and a second computer over a computer network." Appx37(Abstract). The '181 patent claims priority to applications filed in the late 1990s. Appx37(Abstract). VirnetX's predecessor filed the applications leading to the '181 patent at a time when "[a] tremendous variety of methods ha[d] been proposed and implemented to provide security and anonymity for communications over the Internet." Appx88(1:28-30).

In general, communication over the internet follows the Transmission Control Protocol / Internet Protocol (TCP/IP) format, in which every computer has a unique IP address for others to identify. IP addresses are long strings of numbers, which can be difficult to remember, so people use domain names, which are words (e.g., www.apple.com). Domain name servers (DNS) match domain names with IP addresses. Appx106(38:54-56).

The '181 patent describes an approach for establishing a "secure communication link" using secure domain name servers (SDNS) to match "secure top-level domain name[s]" with corresponding secure network addresses. Appx112-13(50:6-51:15). The patent provides an example that "secure top-level domain name[s]" can be based on a non-standard top-level domain name—for example, the ".com" top level domain name could be replaced with ".scom" top-level domain name, "where the 's' stands for secure." Appx112(50:12-16).

Claims 1 and 2 are representative, and their full text is reproduced for convenience on the inside front cover of this brief. Claims 24, 26, 28, and 29 are also independent claims.

B. Prior Art

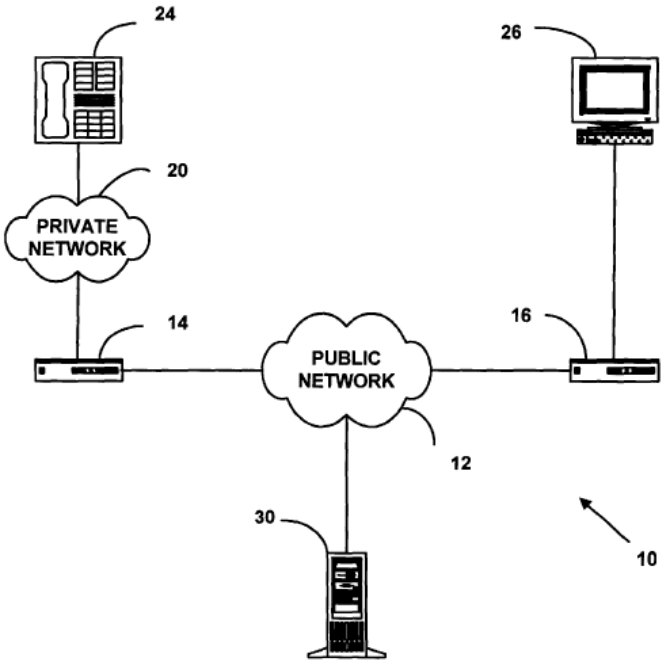
Three prior art references are relevant to this appeal.

1. Beser

The Beser reference, U.S. Patent No. 6,496,867, describes a system and method for establishing secure communication links between two endpoint devices over a public network like the Internet by "tunneling" between the two devices. Appx580(Abstract); Appx602(7:62-8:20). Virtual "tunnels" are a known way of protecting the identity of devices communicating over the Internet by "increas[ing]

the security of communication." Appx580(Abstract); Appx599(1:27-28, 2:8-12); Appx601-02(6:58-7:5). As shown in Figure 1, Beser includes originating (24) and terminating (26) end devices, a first network device (14), a second network device (16), and a trusted third-party device (30):

FIG. 1



Appx582(Fig. 1).

To create a virtual tunnel, *Beser's* originating end device sends a request to initiate a tunneling association, which is received at the first network device. Appx600(4:7-52); Appx602(7:64-66, 8:21-25). The request contains a "unique identifier" (e.g., a domain name) associated with the device with which the originating end device wishes to

establish a tunnel, *i.e.*, the terminating end device. Appx602(8:1-3); Appx603-04(10:37-11:8). The first network device determines if the request is for a destination requiring a secure tunnel and forwards the request, where it is received by the trusted third-party device, which can also be a DNS. Appx600(4:9-11); Appx602(8:3-4, 8:21-22); Appx602-03(8:55-9:1); Appx604(11:32-36).

The trusted third-party device evaluates the request and associates the unique identifier with the second network device by, for example, using a database or directory of subscribers that correlates each unique identifier with the IP addresses of the second network device and the terminating end device. Appx602(8:4-9); Appx604(11:2-5, 11:26-58). After making the association, the trusted third-party device "negotiate[s]" with the first and second network devices to exchange private IP addresses for the end devices. Appx602(8:9-15); Appx603(9:6-11, 9:26-30). The negotiation is carried out by exchanging IP packets that only use the public IP addresses of the network devices or the trusted third-party device in the header fields. Appx604(12:6-13, 12:55-58). In this way, the public and private IP addresses of the end

devices remain hidden even though the negotiation occurs over a public network. Appx604(12:13-19).

Beser explains that the IP packets exchanged during this negotiation "*may require encryption*" for additional protection. Appx607(18:2-5) (emphasis added); *see also* Appx599(1:20-25); Appx608(20:11-14); Appx604(11:22-25).

Following the negotiation, the originating and end devices receive private IP addresses assigned to each end. Appx609(21:48-62). The end devices may thereafter use those private IP addresses to send IP packets, ensuring their identities remain secure. Appx599(2:36-40); Appx602(8:15-20); Appx609(21:55-62).

Beser avoids hacking problems by hiding the identities of the originating and terminating ends of the tunneling association. Appx580(Abstract); Appx599(1:54-58, 2:1-5, 2:36-40); Appx604(12:13-16). Beser also indicates that its tunneling scheme is compatible with, and may supplement, other known security techniques, such as the conventional IPsec protocol, which can use encryption to set up and manage secure IP tunnels. Appx599(1:54-58, 2:1-5, 2:12-14).

Although Beser acknowledges that the use of encryption in certain data-heavy scenarios (e.g., streaming audio or video) may potentially cause challenges because of computational power needed to encrypt and decrypt information "on the fly," Appx599(1:58-63, 2:15-17), it recognizes encryption is routinely used in IP tunnels, in addition to obfuscation of the IP addresses of the originating and terminating devices. Appx599(2:8-14). Indeed, Beser recommends encrypting IP packets exchanged according to its tunneling scheme. Appx604(11:22-25); Appx607(18:2-5); Appx608(20:11-14).

2. Mattaway

The Mattaway reference, U.S. Patent No. 6,131,121, discloses "[a] communication utility for establishing real-time, point-to-point communications between processes over a computer network," including an "apparatus for directly establishing a communication link with the client process upon receipt of the network protocol address from the server." Appx616(Abstract). Mattaway allows for visual and audio communication over the internet. Appx656(25:32-34). To do so, Mattaway discloses a first processing unit 12 connected to a second

processing unit 22, through the internet 24 as shown in Figure 1 (below):

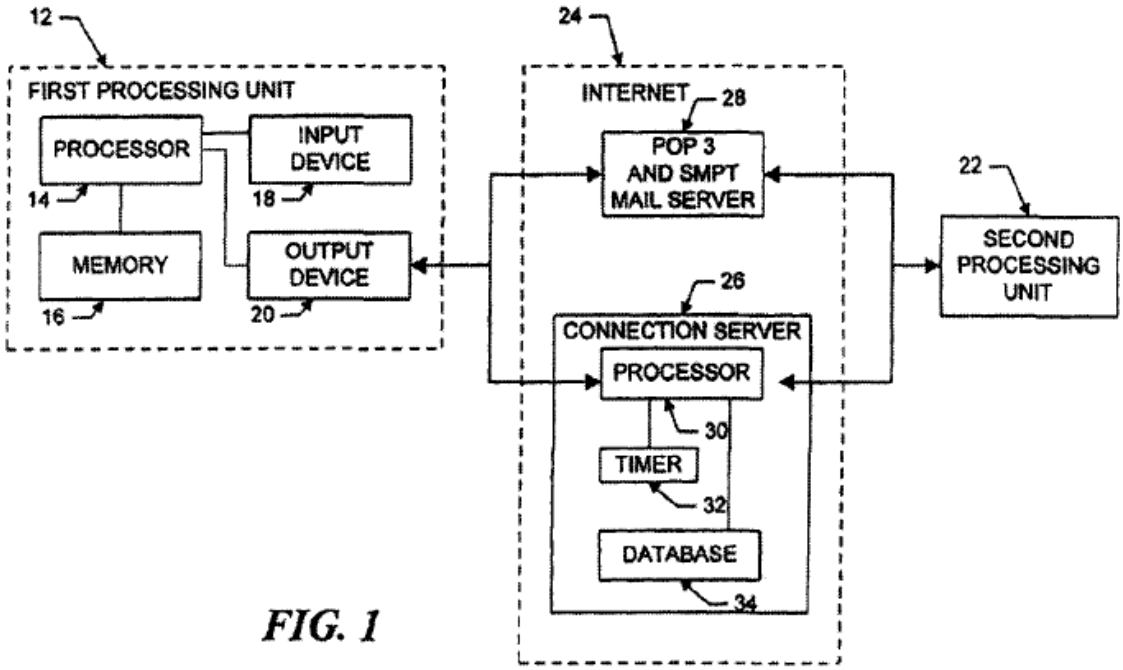


FIG. 1

Appx617.

Connection server 26 provides a "directory information service," allowing for "one-to-one mapping between an identifier of a WebPhone client process, such as an E-mail address, and the current IP address, dynamic or fixed, associated with that WebPhone client process." Appx652(18:19-29); Appx649(12:41-48); Appx652(17:25-31). Connection server 26 may be placed behind a firewall. Appx652(17:44-54; 18:19-29). Similarly, a user may enter "the name or alias or IP address" of the

party to be reached and may store such information on a "personal information directory." Appx649(11:13-20); Appx656(26:39-67).

As shown above, the connection may be established through either (1) a query to connection server 26 or (2) via email, through mail server 28. Appx647-48(7:14-9:40). Querying the connection server returns the IP address of the callee (second processing unit 22), allowing a direct point-to-point connection between the caller (first processing unit 12) and the callee. Appx647(7:24-36). When the connection is made via email, processing unit 12 sends a <ConnectReq> message, which includes its IP address and session number. Appx647-48(7:54-9:28). The second processing unit 22 then extracts the IP address and session number, responding with a <ConnectOK> message including the session number and a temporary IP address. Appx647-48(7:54-9:28). Then, first processing unit 12 responds with a <Call> signal. Appx647-48(7:54-9:28). This may all be done without user input. Appx648(9:29-40). In both cases, the connection allows for "real-time, telephone quality, encrypted audio communication over the Internet and other TCP/IP based networks." Appx656(25:32-34). Connections can be made over a plurality of protocols including Internet Protocol (IP),

Transmission Control Protocol (TCP), RealTime Protocol (RTP), and User Datagram Protocol (UDP). Appx646(6:37-45); Appx652(17:1-6).

3. Provino

The Provino reference, U.S. Patent No. 6,557,037, describes "systems and methods for easing communications between devices connected to public networks such as the Internet and devices connected to private networks." Appx960(1:14-16). These communications may include transfer of a variety of information including "Web pages or the like." Appx962(5:10-13, 5:28-32). In particular, Provino discloses a network 10 which includes a virtual private network (VPN) 15 that includes a firewall 30, servers (including a secure server 31(s) and a name server 17), as well as client devices 12(m), all interconnected by communication link 33. Appx962(6:15-19); Appx964(9:32-10:33); Appx959(Fig. 1). An example of Provino's system is illustrated below (Fig. 1):

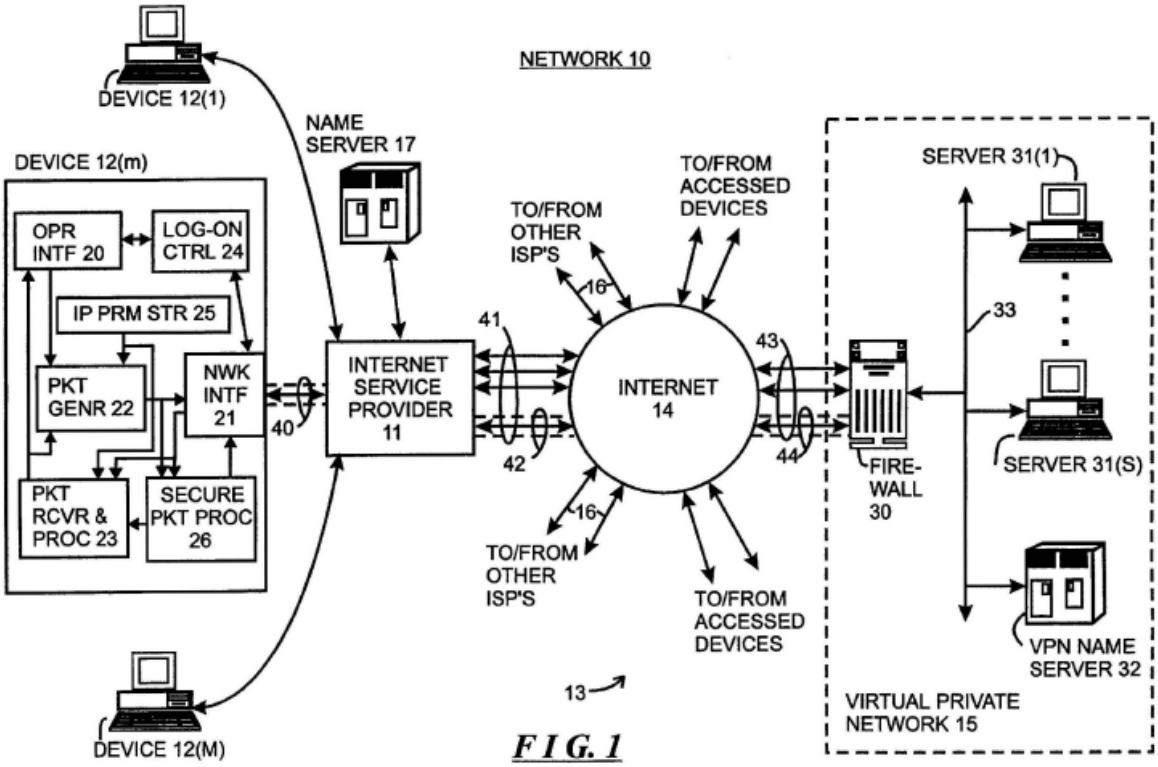


FIG. 1

Appx959.

Provino describes a two-phase process for client device 12(m) to communicate with secure server 31(s), located within VPN 15. Appx965(11:66-12:16). Firewall 30 limits access to server 31(s) by computers outside VPN 15. Appx964(9:6-27).

In phase one, device 12(m) queries name server 17 for the address of secure server 31(s). Appx964(9:32-56). Then, device 12(m) negotiates a secure connection with firewall 30 to extend VPN 15 across Internet 14 to include device 12(m) by establishing a secure tunnel between

device 12(m) and firewall 30. Appx965(12:2-4, 12:17-36). This is done when device 12(m) "generates a message packet requesting establishment of a secure tunnel for transfer to the firewall 30." Appx965(12:17-36). Firewall 30 then authenticates the device 12(m), and, if authenticated, provides encryption and decryption algorithms and keys used for establishing the secure tunnel as well as the address of name server 32. Appx964(9:56-60); Appx965-66(12:17-13:2). This message includes an indicator in the header "<SEC_TUN>" which "indicat[es] that the message is being transferred over the secure tunnel." Appx965-66(12:37-13:2).

In phase two, device 12(m) uses the secure tunnel established in phase one to communicate with name server 32 to resolve the domain name of secure server 31(s) into an integer internet address. Appx964(10:45-67); Appx965(12:8-16); Appx966(13:31-40). In so doing, device 12(m) first contacts conventional name server 17, the DNS associated with ISP 11. Appx963(7:37-43); Appx965(11:5-11). However, "[s]ince nameserver 17 is outside of the virtual private network 15 … [,it] will not have the information requested by the device 12(m)" and will so indicate. Appx965(11:11-13). Upon receipt of this message,

device 12(m) will send "a request message packet" to name server 32, across firewall 30, which will return the requested integer internet address. Appx965(11:11-20, 12:8-16). "Thereafter, the device [12(m)] can use the integer Internet address in generating message packets for transmission to the server 31(s) which is associated with the human-readable Internet address." Appx964(9:6-13); Appx967(15:21-30, 15:27-30); Appx961(3:20-23). In addition to the human readable domain name of secure server 31(s), the method of Provino works with "any form of secondary or informal network address arrangements." Appx967(16:9-17).

C. Reexamination Proceedings

On March 28, 2012, Apple filed a request for *inter partes* reexamination of the '181 patent, challenging every claim as unpatentable in view of twelve asserted references. Appx128-29, Appx132-141. On June 4, 2012, the PTO issued an order granting reexamination of all 29 claims of the '181 patent accompanied by an Office action that adopted 11 of the 13 grounds for rejections presented in the request and rejecting all claims. Appx122-127; Appx1780-1804.

The Examiner found every claim of the '181 patent unpatentable based on the following references:

'181 Patent Claims	Grounds of Rejection
1-12, 14, 15, and 17-29	Anticipated by Beser
1, 2, 7-9, 12-17, 19-21, and 24-29	Anticipated by Mattaway
1-15, 18-23, and 28-29	Anticipated by Provino
1-29	Anticipated by ITU-T H.323 ("Packet-based multimedia communications systems")
1-9, 12-15, and 18-29	Anticipated by Lendenmann, "Understanding OSF DCE 1.1 for AIX and OS/2," October 1995
1-16 and 18-29	Obvious based on U.S. Patent No. 6,499,108 to Johnson in view of RFC 2131 ("Dynamic Host Configuration Protocol"), RFC 1034 ("Domain Names – Concepts and Facilities"), and RFC 2401 ("Security Architecture for the Internet Protocol")
3-4, 10-11, 18, and 23	Obvious based on Mattaway in view of Beser
10 and 11	Obvious based on Mattaway in view of RFC 2401
10, 11, and 17	Obvious based on Lendenmann in view of Beser

’181 Patent Claims	Grounds of Rejection
10 and 11	Obvious based on Lendenmann in view of RFC 2401
24-26	Obvious based on Provino in view of H.323

Appx39; Appx121-Appx439; Appx1805-Appx1820.

On September 4, 2012, VirnetX responded to the Office action in which it argued, among other things, that the broadest reasonable interpretation of “secure communication link” required encryption. Appx1913-14. VirnetX also submitted declarations from Dr. Angelos D. Keromytis and Dr. Robert Dunham Short III, one of the named inventors of the ’181 patent. VirnetX did not amend the claims. Appx1899-2058.

On January 16, 2013, the Office issued an Action Closing Prosecution, maintaining eleven separate rejections. Appx2196-307. Addressing VirnetX’s arguments, the Examiner found Beser disclosed the receiving step of Claim 1 because “transmission of messages, albeit through one or more intermediary devices, is still transmission of a message between a ‘first device’ and a ‘second device’, as claimed.” Appx2213-14. Similarly, the Examiner determined Beser “specifically

teaches utilization of encryption in combination with the tunneling" in its disclosure of a secure communication link. Appx2215-18.

The Examiner also found the secure name of the '181 patent could be "as simple as a telephone number," and found Mattaway disclosed this element through elements protected by its firewall. Appx2228-29. The Examiner likewise found the process of Mattaway was indeed automatic. Appx2234-36. Similarly, the Examiner determined Mattaway disclosed "multiple sessions" as required by claim 13. Indeed, each call had a unique "session ID number." Appx2236-37. Regarding Provino, the Examiner found use of a secure name, "the domain name associated with a given VPN server" (e.g. element 31(s)), and an unsecured name, "the domain name of firewall 30," associated with "each of the VPN servers," (e.g. element 31(s)). Appx2267-68.

VirnetX and Apple filed comments following the Action Closing Prosecution. Appx2381-2437; Appx2456-2505. On August 16, 2013, the Examiner issued a Right of Appeal Notice that maintained the rejection of all claims. Appx2535.

Both VirnetX and Apple requested an oral hearing before the Board. Appx5048-49. VirnetX later withdrew its request for a hearing,

but stated that it "plan[ned] to participate" when an oral hearing was scheduled. Appx5182. On September 11, 2015, the Board held an oral hearing. Appx5190-5219. VirnetX did not appear. Appx5190-Appx5192.

D. The Board's Decision

The Board's final decision found claims 1-12, 14, 15, and 17-29 anticipated by Beser; claims 1, 2, 7-9, 12-17, 19-21, and 24-29 anticipated by Mattaway; and claims 1-15, 18-23, 28, and 29 anticipated by Provino. Appx13, 24, 28, 34. The Board did not address the eight other rejections maintained by the Examiner in the Right of Appeal Notice, including that all the claims were also anticipated and/or rendered obvious by six additional references. Appx2535-2545. Because the Board found the claims anticipated by Beser, Mattaway, and Provino, it concluded it was unnecessary to address VirnetX's arguments regarding secondary considerations, but the Board nonetheless observed that in a related proceeding it had found VirnetX's secondary consideration evidence "insufficient to outweigh the evidence of obviousness." Appx34.

1. The Board's Claim Constructions

Applying the broadest reasonable interpretation standard required in reexaminations, the Board construed three terms, (a) "A Secure Name," (b) "An Unsecured Name," and (c) "A Secure Communication Link." Appx7–12.

a. "A Secure Name"

The Board determined that "a secure name" includes "a name that connotes a level of security, including corresponding to a secure computer network address." Appx10. The Board rejected VirnetX's argument that a "secure name … 'is a name used to communicate securely that is resolved by a secure name service (i.e., a service that both resolves a name into a network address and further supports establishing a secure communication link),'" finding the '181 patent and VirnetX's expert Dr. Keromytis' declaration insufficient to support VirnetX's proposed construction of "secure name." Appx8. The Board concluded the portion of the '181 patent relied on by VirnetX "[did] not discuss or explain what a secure name itself is" and Dr. Keromytis provided "no underlying support for his understanding." Appx8. Instead, the Board relied on the '181 patent's clear statement that "'*any* other non-standard top-level domain name' can be used to replace the

top-level domain name of server 3304," as well as VirnetX's own prior statements to the PTO that a "secure name" could be as simple as a telephone number, to conclude that "secure name" should be broadly construed as "a name that connotes a level of security." Appx9; *see also* Appx2229. Nonetheless, the Board also observed that "the prior art satisfies [VirnetX's] narrow construction." Appx9.

b. "An Unsecured Name"

The Board determined that "an unsecured name" includes "a name that does not connote a level of security, including corresponding to an unsecured computer." Appx10. The Board rejected VirnetX's argument that "an unsecure[d] name" is a name that "does not require resolution by a secure name service" because the portions of the '181 patent cited by VirnetX "do not address what an unsecured name is" and Dr. Kermoytis' declarations also failed to support VirnetX's construction because those declarations "do not discuss 'an unsecured name' as recited and provide insufficient support for [VirnetX's] understanding." Appx10.

c. "A Secure Communication Link"

The Board determined that the broadest reasonable interpretation of "a secure communication link" is "a transmission path that restricts

access to information on its path using one or more of various techniques, including obfuscation methods that hide the information on the path, such as, encryption, address hopping, and authentication." Appx12. The Board rejected VirnetX's argument "that '[t]he broadest reasonable interpretation of the recited secure communication link requires encryption,'" finding it unpersuasive and not supported by the '181 patent's specification. Appx10-11.

First, considering VirnetX's arguments based on the '181 patent's specification, the Board noted that "[a]lthough the '181 patent discusses encryption in the context of data security …, the disclosure states '[d]ata security is *usually* tackled using some form of data encryption' … and also states that '[a] tremendous *variety of methods* have been proposed and implemented to provide security … .'" Appx10-11 (citing Appx88(1:28-29))(emphasis added). The Board further observed that the '181 patent discusses a secure communication link that is not limited to encryption. Appx11(citing Appx112(50:1-3)).

Second, the Board considered this Court's decision in *VirnetX, Inc. v. Cisco Systems, Inc.*, 767 F.3d 1308 (Fed. Cir. 2014), which involved this term in a related patent. The Board cited this Court's recognition

that "'encryption is just one *possible* way to address data security.'" Appx11 (quoting *Cisco*, 767 F.3d at 1323). And while recognizing that in *Cisco* the Court concluded that a secure communication link requires both data security and anonymity, the Board noted that in this reexamination proceeding the claims were to be given the broadest reasonable construction and neither VirnetX nor Apple were arguing that the Board should adopt *Cisco*'s construction of secure communication link. Appx11-12. Finally, the Board observed that even under the narrower construction adopted in *Cisco*, the Court had also found that encryption was not *always* required to provide security, but that security could come instead by physical security. Appx12.

Accordingly, the Board determined "'a secure communication link' may include but does not require encryption." Appx12. The Board found that "a secure communication link can be created by anonymity or a physical security" and that security can be provided by "various techniques, such as an IP address hopping regime that changes IP addresses in packets." Appx12.

2. The Board's Anticipation Findings

The Board affirmed the Examiner's rejection of claims 1-29 under 35 U.S.C. § 102(e) as anticipated by *Beser*, *Mattaway*, and/or *Provino*. Appx13; Appx24; Appx28; Appx34.

a. Beser

The Board concluded *Beser* anticipated claims 1-12, 14, 15, and 17-29. Appx13. The Board rejected VirnetX's argument that the Examiner had improperly mapped "two separate devices in Beser (e.g., 14/24 and 16/26) to the recited first and second devices in claims 1 and 2" of the '181 patent, finding that VirnetX mischaracterized the Examiner's rejection and that what the Examiner actually concluded was that either of these devices in each set would meet the claim limitations. Appx14. The Board determined that the Examiner's rejection was consistent with the specification, which specifically contemplated "embodiments where the first device … includes more than one element or structure." Appx15. The Board also rejected VirnetX's argument that the Examiner changed his position regarding what constituted the "secure name," changing between a "private IP address when packetized and a unique identifier of the telephony device 26." Appx15-16. Instead, the Board agreed with Apple that the

Examiner, in fact, had been consistent in finding that "the unique identifier of a telephony device (e.g., 26) in Beser is the recited 'secure name.'" Appx16. The Board concluded that Beser's unique identifier was a secure name because it serves to hide the identity of the terminating devices "on the public network, ensuring anonymity," and thus "is a name used to create and connote a level of security." Appx17. Moreover, the Board found the encrypted packets disclosed in Beser added security by ensuring that the unique identifier could not be read on the public network. Appx17.

Third, the Board rejected VirnetX's argument that "the Examiner … overlook[ed] specific requirements of the claims" in finding that Beser met the claimed steps of sending and receiving a message. Appx18. The Board noted that "claim 1 does not recite the message is received at any particular device or cannot be transmitted through an intermediary device" and concluded Beser disclosed this step in two places. Appx19-20.

Finally, the Board rejected VirnetX's arguments related to whether Beser anticipated claims 2, 4, 9, 10, 11, and 24. Appx21-24. The Board found that VirnetX's arguments were based on an incorrect

reading of the claims of the '181 patent as well as a misreading of what Beser discloses.

b. Mattaway

The Board concluded that Mattaway anticipated claims 1, 2, 7-9, 12-17, 19-22, and 24-29. Addressing claim 1, the Board rejected VirnetX's argument that "Mattaway does not disclose a first device associated with a secure name and unsecured name," finding Mattaway's email addresses are secure, in part because they are placed behind a firewall. Appx24-25. The Board also noted the email addresses can be encrypted, providing additional security. Appx25. The Board found the associated name or alias of the first device, which initiates the call, is exposed to the receiver of the call, thereby making it unsecure. Appx26.

Second, the Board rejected VirnetX's argument that use of data security techniques such as encryption or a firewall were not sufficient to create a secure name. Appx26. The Board was "not persuaded" by VirnetX's arguments that the '181 patent "disparages" these techniques and that they therefore did not create a secure name. Appx26.

Third, the Board dismissed VirnetX's argument "that Mattaway's <CONNECT REQ> message is not a message received at the network address corresponding to the secure name associated with the first device as recited in claim 1" because that was not the basis of the Examiner's rejection. Appx27-28. Instead, the Examiner's rejection was based on the <CALL> message, which goes from "a second device (e.g., webphone 1536) at a network address related to or corresponding with a secure name associated with the first device (e.g., email address is correlated to the IP address of webphone 1538)." Appx27-28.

With respect to the remaining claims, VirnetX did not make any independent arguments for patentability over Mattaway but instead referred back to its arguments for claim 1. Appx2291-92. The Board accordingly determined that Mattaway anticipated claims 1, 2, 7-9, 12-17, 19-22, and 24-29. Appx28.

c. Provino

The Board concluded that Provino anticipated claims 1-15, 18-23, 28, and 29. Appx28. Addressing claim 1, the Board rejected VirnetX's argument that the Examiner improperly mapped different elements of *Provino* to the first and second devices and "switched positions

throughout the proceedings," finding instead "the Examiner mapped server 31(s) to the first device and device 12(m) to the recited 'second device' in claim 1." Appx28; Appx30. The Board noted that the Examiner had adopted Apple's reexamination Request, which "discuss[ed] server 31(s) connecting to device 12(m) and two names associated with server 31(s)." Appx30 (citing Appx288). And the Board concluded that it even if there was "some apparent, conflicting mapping by the Examiner to the claimed first and second devices as recited in claims 1 and 2," it should give "some latitude in the rejection and in clarifying the position the rejection takes" because VirnetX's claims themselves switch the meaning of the same terms used in claims 1 and 2, which "only contributes to the confusion." Appx29. As the Board explained, VirnetX "labels the *first* device in claim 1 as the device that is associated with the secure name and then switches in claim 2 to label a *second* device having a secure name." Appx29.

Second, the Board rejected VirnetX's argument that Provino "does not disclose 'a first device associated with a secure name and an unsecured name' as recited in the preamble of claim 1," because this argument also failed to address the Examiner's rejection. Appx30. The

Board further rejected VirnetX's argument that, even if server 31(s) is mapped to the first device, server 17 does not contain any name associated with server 31(s), finding that VirnetX ignored several other components of Provino that allow for a message to be received by 31(s) from 12(m). Appx30-31. The Board mapped Provino's server31(s) to the "secure name" of the first device because it is "not accessible to servers (e.g., nameserver 17) and is located behind a firewall, which connotes a level of security for the name." Appx31.

Third, the Board rejected VirnetX's argument that "nameserver 32 in Provino operates in a conventional manner that is disclaimed by the '181 patent," finding that a secure name "need not be resolved by a secure name server" and that VirnetX did not disclaim the use of a server in assisting the communication link of claim 1. Appx31-32. The Board found that, "even presuming such a disclaimer exists," server 32 "is not a standard DNS server on the public Internet" but is instead "located internal to VPN 15." Appx32. The Board found Provino "establishes a secure communication link due to the firewall and encryption/decryption algorithms." Appx32.

Fourth, the Board rejected VirnetX's argument "that the domain name stored in nameserver 17 is not any name, including an unsecured name, associated with the first device (e.g., server 31(s))," finding that "[b]oth servers 17 and 32 contain the human readable Internet addresses and an integer Internet address for devices" and that Provino further "discloses access to an unsecured name (e.g., integer Internet address) through a public domain name server (e.g., 17)." Appx32 (citing Appx963(8:40-43, 8:67-9:5)). As with its analysis of Beser, the Board determined that "the recited 'first device' is not limited to one element in Provino" and that, "[a]s such, multiple components of the VPN (e.g., firewall 30, sever 31(s)) can be mapped to the recited 'first device' in claim 1." Appx33.

As with the rejection based on Mattaway, VirnetX did not make any independent arguments for the patentability of the remaining claims but instead relied on its arguments for claim 1. Because the Board rejected VirnetX's arguments for claim 1, the Board concluded that Provino anticipated claims 2-15, 18-23, 28, and 29. Appx. 34.

3. Remaining Rejections

Because the Board found that Beser, Mattaway, and Provino anticipated all the claims of the '181 patent, it concluded it was unnecessary to reach the eight other rejections that also invalidated the claims, including the Examiner's finding that all the claims were obvious even if not anticipated. Appx34. Nonetheless, the Board briefly addressed VirnetX's arguments about secondary considerations of obviousness, which relied on the declaration of inventor Robert Short—the same declaration that VirnetX now cites for the purported background of the invention. VirnetX Br. 6-9. The Board explained that it did not need to address secondary considerations "because the rejections discussed are based on anticipation and covering all the rejected claims." Appx34. Nonetheless, the Board noted that in a related proceeding, it "found the evidence insufficient to outweigh the evidence of obviousness." Appx34 (citing *Cisco Sys., Inc. v. VirnetX, Inc.*, Appeal No. 2014-000591, 2014 WL 1322692 (PTAB April 1, 2014)).

SUMMARY OF THE ARGUMENT

The Board correctly affirmed the Examiner's rejection of claims 1-29 of the '181 patent because, after thoroughly examining just three of the nine references relied on by the Examiner, the Board found that

every claim was anticipated and that most of the claims were anticipated by all three references. None of VirnetX's arguments overcome the Board's overlapping grounds for finding all the claims unpatentable.

First, VirnetX fails to show that the Board erred in ascertaining the broadest reasonable interpretation of the "secure communication link," "secure name," and "unsecured name" terms. The Board appropriately rejected VirnetX's proposed constructions of these terms because VirnetX's constructions attempted to improperly limit the terms to specific embodiments. In particular, for the "secure communication link" term, VirnetX seeks again to have this Court find that encryption is always required, despite clear recognition in the '181 patent that security does *not* have to come from encryption. And for the "secure name" and "unsecured name" terms—which appear *nowhere* in the specification of the '181 patent—VirnetX attempts to deviate from the clear breadth of these terms by limiting them to a narrow requirement that they be a name resolved/not resolved by a "secure name service," even though that construction has no support in the '181 patent.

Second, VirnetX's challenge to the Board's finding that Beser anticipates is thoroughly flawed. VirnetX fights the Board's finding that Beser discloses a "first device" and "second device," arguing that the Board improperly combined multiple devices of Beser to find the "first" and "second" devices. But this is wrong on the facts and the law. As a matter of fact, the Board identified single components in Beser that qualify as the "first" and "second" devices. And as a matter of law, the Board was entirely correct under Federal Circuit precedent that multiple components in Beser performing functionalities intended to work together can be considered to meet the generic claim term "device." VirnetX's remaining challenges largely hinge on its erroneous claim constructions that the Board properly rejected.

Third, VirnetX's cursory challenges to the Board's finding that Mattaway anticipates are based on its flawed reading of Mattaway's disclosure and its erroneous claim constructions that, for instance, would limit "secure name" to one narrow embodiment in the '181 patent. In addition, although VirnetX contends that the Board relied on a "new grounds" of rejection in finding that Mattaway disclosed a "message … of the desire[] to securely communicate," the reality is

VirnetX distorts what the Examiner had actually decided—and what the Board ultimately affirmed.

Finally, VirnetX makes only perfunctory arguments regarding the Board's findings that Provino anticipates, despite the fact that Provino alone renders most of the '181 patent's claims unpatentable. VirnetX repeats its legally flawed contention that a "device" must be one *thing*, rather than recognizing the breadth of that term. And VirnetX again relies on its erroneous construction of "secure name." But even if the Board had adopted this erroneous construction, Provino discloses all elements. VirnetX has shown no error—let alone a lack of substantial evidence—in the Board's findings that Provino anticipates.

STANDARD OF REVIEW

The Board's anticipation determinations are questions of fact reviewed for substantial evidence. *In re Rambus, Inc.*, 753 F.3d 1253, 1256 (Fed. Cir. 2014). "Substantial evidence" is a deferential standard of review that the Supreme Court has analogized to a court's review of a jury's fact findings. *Universal Camera Corp. v. NLRB*, 340 U.S. 474, 477 (1951).

This Court reviews "the Board's ultimate claim constructions de novo" and any "underlying factual determinations involving extrinsic evidence for substantial evidence." *Microsoft Corp. v. Proxyconn, Inc.*, 789 F.3d 1292, 1297 (Fed. Cir. 2015) (citing *Teva Pharms. U.S.A., Inc. v. Sandoz, Inc.*, 135 S. Ct. 831, 841-42 (2015)). During reexamination, the Board gives claims of unexpired patents their broadest reasonable interpretation. *In re Am. Acad. of Sci. Tech Ctr.*, 367 F.3d 1359, 1364 (Fed. Cir. 2004). This Court, in reviewing those claim constructions, determines whether the Board's constructions are reasonable. *In re NTP, Inc.*, 654 F.3d 1279, 1287 (Fed. Cir. 2011).

ARGUMENT

I. The Board Correctly Construed the Claims

A. A "Secure Communication Link" Does Not Require Encryption

VirnetX argues that "[t]he broadest reasonable interpretation of the recited secure communication link requires encryption." Appellant Br. 27. This is the same argument VirnetX has raised—and the Board has consistently rejected—in proceedings involving patents in the same family as the '181 patent. *See Apple Inc. v. VirnetX Inc.*, IPR2014-

00237 (Paper No. 41) (May 11, 2015); *Apple Inc. v VirnetX Inc.*, IPR2014-00238 (Paper No. 41) (May 11, 2015).

The reason why different panels of the Board have been correct in consistently rejecting VirnetX's proposed construction is simple: There is no basis in the specification for finding that a secure communication link *always* requires encryption, as opposed to other forms of data security. For example, VirnetX references the "Tunneled Agile Routing Protocol" (TARP) as "*embodiments* with 'a unique two-layer encryption format … .'" VirnetX Br. 29. But VirnetX nowhere suggests that this embodiment is limiting. Likewise, VirnetX notes that encryption may "*provid[e]* data security" and "the secure communication link *may* be established without the need for a user to manually enter encryption keys," but none of this means encryption is the *only* way to achieve data security. VirnetX Br. 27-28. In fact, the passages VirnetX cites for support are limited to "an embodiment" or "one embodiment" of the invention, Appx91(8:9-10); Appx92(9:57-58); Appx93(11:5-7), and a reference to the establishment of the secure communication link being automatic. Appx112(50:1-3); *Trading Techs. Int'l, Inc. v. eSpeed, Inc.*, 595 F.3d 1340, 1352 (Fed. Cir. 2010).

Indeed, in a passage quoted in VirnetX's own brief, the '181 patent explains that "[d]ata security is *usually* tackled using some form of data encryption," VirnetX Br. 27 (quoting Appx88(1:50-57)), which is a far cry from saying it *must* be used to establish a secure communication link in the context of the claims.

And other parts of the '181 patent make clear that encryption is not required to provide data security. As the Board observed, the '181 patent recognizes that "[a] *tremendous variety of methods* have been proposed and implemented to provide security … ." Appx10-11 (citing Appx88(1:28-29)). For example, the '181 patent explains that a secure communication link can be established using techniques like IP address hopping. Appx112(50:42-56). In rejecting VirnetX's proposed construction, which would always require encryption to be used in a secure communication link, the Board noted that this Court, in considering similar passages of a related patent, found "'that encryption is a narrower, more specific requirement than security.'" Appx11 (citing *Cisco*, 767 F.3d at 1323).

VirnetX relies heavily on a statement by its expert, Dr. Keromytis, that a person of ordinary skill in the art would have understood the

claimed "secure communication link" in the '181 patent to require encryption. VirnetX Br. 28. The Board, however, rightly rejected VirnetX's attempt to use extrinsic evidence to narrow the broadest reasonable interpretation of the claim. Moreover, Dr. Keromytis identified no basis for his conclusion other than simply his say-so. Appx 3055(¶27) Such "conclusory, unsupported assertions by experts as to the definition of a claim term are not useful to a court." *Phillips v. AWH Corp.*, 415 F.3d 1303, 1318 (Fed. Cir. 2005) (en banc).

Also notably missing from VirnetX's proposed construction before the Board, as well as this Court, is any explanation of what it means for a secure communication link to "require encryption." For example, encryption can be used during the initial exchanges that set up a secure communication link, or during the transmission of data after the link has been established. In the latter case, all of the data being transmitted may be encryption, or only portions of the packets that carry data. And there is no dispute that the Beser, Mattaway, and Provino references shows use of encryption in various ways. Ultimately, VirnetX's exaggerated emphasis on the necessity of encryption is irrelevant in this appeal.

VirnetX argues the Board "attempted to side-step" this Court's decision in *Cisco* and that the Board stated it could "ignore" this Court's claim construction. VirnetX Br. 29. Not so. The Board considered *Cisco* and concluded that it supported the Board's broadest reasonable interpretation of "secure communication link." Appx11-12. In fact, VirnetX mischaracterizes this Court's decision in *Cisco*, contending "this Court observed" that "the specification discloses no embodiment where both data security (*ensured through encryption*) and anonymity are not required." VirnetX Br. 29 (citing *Cisco*, 767 F.3d at 1318) (emphasis omitted and added). But *not once* did this Court state that data security was "ensured through encryption." Its observations on encryption and security actually make clear the opposite—the Court stated "that encryption is a narrower, more specific requirement than security" and "that encryption is just one possible way to address data security." *Cisco*, 767 F.3d at 1323. Indeed, VirnetX itself told this Court that "encryption is not the only means of addressing data security" and that physical security measures could provide security. *See Br. of Appellee VirnetX, Inc.* in *VirnetX, Inc. v. Cisco Sys., Inc.*, No. 2013-1489 (Fed. Cir.) at 39-40. In that context, applying the *Phillips*

standard, the Court construed "secure communication link" as used in the claims of a related patent to be "a direct communication link that provides data security and anonymity." *Cisco*, 767 F.3d at 1319.

Further, VirnetX misreads this Court's analysis in *Cisco*. In *Cisco*, the district court had construed a secure communication link as requiring data security, and the issue on appeal before this Court was whether secure communication link "require[s] *not only* data security *but also* anonymity." *Cisco*, 767 F.3d at 1317. The point in *Cisco* was that, under the *Phillips* standard used by a district court, a secure communication link has to have both data security and anonymity.[1] But as is clear from the decision, *Cisco* did *not* state that an anonymity technique cannot provide a form of data security. And ultimately that is what the Board recognized—that a secure communication link is created by "restrict[ing] access to information." Appx12.

That is also the construction that corresponds to the '181 patent's specification. Indeed, even VirnetX acknowledges the breadth of the

[1] This Court has explained that the broadest reasonable interpretation used in a reexamination proceeding can differ from a correct construction under *Phillips*. *PPC Broadband, Inc. v. Corning Optical Commc'ns RF, LLC*, 815 F.3d 734, 743 (Fed. Cir. 2016).

term "security" as it is used in the specification; it argues elsewhere that "'security' within the '181 patent's specification means different things in different scenarios." VirnetX Br. 31. The Board's construction of secure communication link thus correctly captures the breadth of VirnetX's use of security throughout the '181 patent's specification.

Thus, far from "ignor[ing]" the *Cisco* decision, the Board expressly relied on it to reject VirnetX's argument that a secure communication link requires encryption. Appx11-12. The Board thus followed this Court's instruction and expressly considered the construction of secure communication link in *Cisco*. *See Power Integrations, Inc. v. Lee*, 797 F.3d 1318, 1326 (Fed. Cir. 2015).

Regardless, "[t]here is no dispute that the [B]oard is not generally bound by a prior judicial construction of a claim term." *Id.* The Board here did not adopt for this reexamination proceeding *Cisco's* construction of secure communication link for two reasons: First, unlike in a district court proceeding, a claim in reexamination is given its broadest reasonable interpretation. Appx12; *Power Integrations*, 797 F.3d at 1326. Second, the Board correctly observed that *neither* VirnetX nor Apple had argued that the broadest reasonable interpretation of "a

secure communication link requires *both* security and anonymity." Appx12 (emphasis added).

In any event, VirnetX does not—and cannot—contest that the broadest reasonable interpretation standard applies to this reexamination proceeding. Instead, VirnetX suggests that the Board's construction is "divorced from the specification and the record evidence." VirnetX Br. 30 (citing *Proxyconn*, 789 F.3d at 1298). It then points to the fact that this Court examined the specification in *Cisco* and contends those findings compel the Board to reach the construction it proposes for the '181 patent. As explained above, the Board specifically considered the intrinsic evidence and the Federal Circuit opinion in arriving at its opinion.

The '181 patent's discussion of security provided by techniques such as IP address hopping also supports the Board's construction of secure communication link as not requiring encryption. Appx12. VirnetX struggles to rebut the Board's reference to these security techniques, asserting that "the embodiment [in the '181 patent] that describes generation of 'a random-number sequence' required for address hopping still requires encryption as a separate safeguard."

VirnetX Br. 31 (citing Appx100(26:10-13); Appx101(27:37-40)). But the portions of the '181 patent that VirnetX citations actually confirm *the opposite* of VirnetX's argument—that encryption is optional. For example, the '181 patent explains that the "sync field" of a hopped packet "*could* appear in the clear *or* as part of an encrypted portion of the packet." Appx100(26:11-13) (emphasis added). The patent further describes *"[o]ne implementation*" that uses an "'inner header' 1306 that is encrypted." Appx101(27:37-40). Although some embodiments may discuss using encryption and addressing hopping together, the patent also references addressing hopping independently of encryption. *See, e.g.*, Appx97(20:51)-Appx98(21:1-2).

Finally, VirnetX argues that the Board should have construed the broadest reasonable interpretation of secure communication link as "requir[ing] encryption" because during prosecution of a related patent VirnetX "disclaimed 'secure communication links' that do not require encryption." VirnetX Br. 32 (citing Appx3181). Notably, VirnetX *itself* never actually asserted to the Board that it had disclaimed links not requiring encryption; rather, VirnetX couched it as an argument *Apple* made in a district court case, in which the *Phillips* standard applied.

See Appx2980 (citing Apple's district court arguments); Appx3181 (Apple's district court claim construction brief). VirnetX cannot fault the Board for not accepting a disclaimer argument that VirnetX never actually argued to the Board. Regardless, the Board was not required to narrow the broadest reasonable interpretation of secure communication link based on VirnetX's self-serving assertion that it had disclaimed anything not requiring encryption. Prosecution history disclaimer "generally only binds the patent owner." *Tempo Lighting, Inc. v. Tivoli, LLC*, 742 F.3d 973, 978 (Fed. Cir. 2014). And VirnetX had an opportunity during the reexamination to *amend* its claims so as to claim that a secure communication link must use encryption. "To the extent [VirnetX] wanted to limit [a secure communication link to require encryption], it could have expressly done so. It did not[.]" *In re Rambus Inc.*, 694 F.3d 42, 47 (Fed. Cir. 2012).

B. A "Secure Name" Is Not Limited to A Name That Is Resolved by A Secure Name Service

VirnetX next argues that a "secure name" should be construed "to require resolution by a secure name service and support for a secure communication link." VirnetX Br. 36. The Board rejected this proposed construction because the passage of the '181 patent that VirnetX cited

to the Board "discusses a secure domain name service (SDNS)" but "does not discuss or explain what a secure name itself is." Appx8 (citing Appx2976)). In fact, the term "secure name" does not appear anywhere in the specification of the '181 patent.

VirnetX also relied on Dr. Keromytis' opinion on the meaning of secure name. But the Board found those opinions unpersuasive because he again failed to provide any "underlying support for his understanding." Appx8.

On appeal, VirnetX argues that its construction "is consistent with the embodiments depicted in Figures 26 and 27 of the '181 patent, in which a secure name service resolves secure names but sends requests for unsecured names to a conventional DNS." VirnetX Br. 35 (citing Appx107(40:33-36)). But even under a *Phillips*-type construction it is improper to limit claims to preferred embodiments identified as such in a patent disclosure. *Trading Techs. Int'l*, 595 F.3d at 1352. And limiting the construction of that term is plainly improper here, in which the broadest reasonable interpretation undisputedly applies.

The cited passages yet again do not support VirnetX's proposed construction of "secure name." Nowhere does the '181 patent's

specification discuss "secure name"—the term is not used outside the patent claims and does not have an accepted meaning in the art.[2] And VirnetX's circular definition—that a "secure name" is one that is resolved by a "secure name service"—cannot be correct; it never resolves the question of what a "secure name" is, or is not.

VirnetX's attempt to impute a meaning by reference to certain "preferred embodiments" in the patent also fails. The portions of the '181 patent cited by VirnetX refer to examples of application of the modified secure domain name service; they do not mention, much less define, "secure name." Appx107(40:15-36). In any event, the '181 patent makes clear that these are *non-limiting* examples. *See* Appx107(40:15-17) ("Gatekeeper 2603 *can be implemented* on a separate computer (as shown in FIG. 26) or as a function within modified DNS server 2602.") (emphasis added) and Appx107(40:29-31) ("FIG 27 shows steps that *can be executed* by DNS proxy server 2610 to handle requests for DNS look-up for secure hosts.") (emphasis added).

---

[2] The term "secure name" is clearly indefinite, but the Patent Office cannot consider indefiniteness grounds in *inter partes* reexamination. 35 U.S.C. § 311 (limiting *inter partes* reexamination to grounds based on prior art).

VirnetX also points to embodiments in which the SDNS is accessed through "secure portal 3010 'in the clear'" or where it is accessed "through secure portal 3010 preferably using an administrative VPN communication link." VirnetX Br. 36 (citing Appx112(50:38-40); Appx113(51:30-32). But these passages merely discuss "prefer[red]" and "alternative[]" embodiments for accessing the SDNS. They do not discuss "a secure name," as used in the claims.

Finally, VirnetX cites the conclusory opinions of Dr. Keromytis on the meaning of "secure name," which repeat VirnetX's circular reasoning that "[o]ne of ordinary skill in the art would have understood that 'secure names' in the context of the '181 patent are those names used to communicate securely that are resolved by a secure name service." Appx3072; *see also* VirnetX Br. 34-35 (citing Appx3066-67; Appx3125). The Board correctly found Dr. Keromytis' circular opinions "not … persuasive" because "no underlying support for his understanding has been provided." Appx8.

The Board correctly construed "secure name" to be "a name that connotes a level of security, including corresponding to a secure computer network address." Appx10.

C. A "Unsecured Name" Is Not Limited to A Name That Does Not Require Resolution by A Secure Name Service

VirnetX argues that an "unsecured name" is "a name that does not require resolution by a secure name service." VirnetX Br. 37. VirnetX claims "[t]hat is how the '181 patent describes unsecured names," but that is wrong because, as with "secure name," the term "unsecured name" appears nowhere in the '181 patent's specification and has no accepted meaning in the art. *Id.*

VirnetX once again points to the embodiments disclosed in Figures 26 and 27, VirnetX Br. 37, but these are non-limiting embodiments—a fact VirnetX concedes. VirnetX Br. 37 ("For example, an unsecured name *may be resolved* by a conventional domain name service … ." (emphasis added)). *Trading Techs. Int'l*, 595 F.3d at 1352 (explaining that broad claim language should not be limited to the only disclosed embodiment "unless the patentee has demonstrated a clear intention to limit the claim scope using 'words or expressions of manifest execution or restriction'"). VirnetX also relies on Dr. Keromytis' opinions. VirnetX Br. 37 (citing Appx3066-67; Appx3125). But, at least in the

passages VirnetX cites, Dr. Keromytis never even refers to an unsecured name.

As the Board correctly observed, the passages of the '181 patent that VirnetX identifies "do not address what an unsecured name is, but rather focus on how a name is resolved by service and establishing a 'non-VPN communication link,' which is not recited in the claims." Appx10.

Accordingly, the Board correctly construed "an unsecured name" as "a name that does not connote security, including corresponding to an unsecure computer network address." Appx10.

II. THE COURT SHOULD AFFIRM THE BOARD'S FINDING THAT BESER ANTICIPATES CLAIMS 1-12, 14, 15, AND 17-29

A. Substantial Evidence Supports the Board's Finding That Beser Anticipates Claim 1

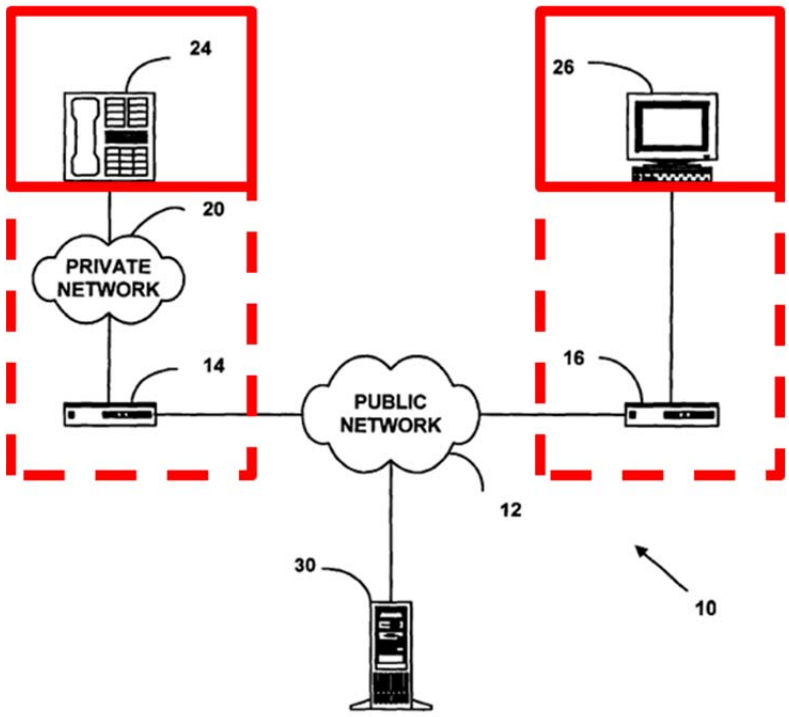
1. Beser Discloses a "First Device" and "Second Device"

VirnetX argues the Board committed legal error by finding "that multiple devices and components from Beser could be combined to anticipate the claimed 'first device' and 'second device.'" VirnetX Br. 38. But tellingly, VirnetX neither quotes nor cites any portion of the Board's decision in which it supposedly made this finding—because this

is *not* what the Board did. Rather, the Board affirmed the Examiner's "mapping either Beser's device 24 or 26 in Figure 1 *alone or in combination* with devices 14 or 16 to the first device or second device as recited in claims 1 and 2." Appx14 (emphasis added).

The Board simply did not, as VirnetX argues, "[c]ollaps[e] multiple devices [of Beser] into one." VirnetX Br. 39. Instead, the Board explained that "there is no physical incorporation of the components in Beser," and the Board concluded the first device and second device could be defined as network devices 24 and 26 or, *alternatively*, the first device and second device could be defined by network device 24 together with network device 14 and network device 26 together with network device 16. Appx14. In other words, boxes identifying the first and second devices could be drawn around only network devices 24 and 26, or could be drawn around network devices 14/24 and 16/26, as depicted below.

FIG. 1



Appx582 (annotations added).

The Board's reasoning is consistent with the flexibility recognized in defining computing or networking devices. For example, a set of operations that provide a defined functionality may be lodged within a single device, or distributed and performed across a set of devices that together provide the specified functionality. In fact, the '181 patent itself recognizes this to be true. Appx107(40:24-28) ("It will be appreciated that functions of DNS proxy 2610 and DNS server 2609 can be combined into a single server for convenience. Moreover, although

element 2602 is shown as combining the functions of two servers, the two servers can be made to operate independently.").

Distributing functions or operations across multiple devices is neither required by Beser nor defeats Beser's purpose. Considering network devices 14 and 24 or 16 and 26 together as the first device and second device does not change or affect the functionality of these network devices or change the operation of Beser's system. Beser explains that network devices 14 and 16 are the interfaces with the public network 12 (e.g., the Internet), and that these network devices can be a variety of devices, including "modified router," "modified gateways," "edge routers," or "cable modems." Appx600(4:7-33). Network devices 24 and 26 are the "originating and terminating ends of data flow" and can be "telephony devices or multimedia devices" or "other types of network devices." Appx600(4:43-54). Beser also discloses that network devices 14 and 24 can be part of the same device, explaining that originating device 24 can be "a phone that is physically connected to the first device 14." Appx603(10:23-28). And, like the '181 patent itself, Beser emphasizes flexibility in configuring the devices that make up the system illustrated in Figure 1. Appx601(5:3-14).

The Board's analysis is entirely consistent with the requirement that an anticipatory reference discloses all the claimed limitations "arranged or combined in the same way as in the claim." *Net MoneyIN, Inc. v. VeriSign, Inc.*, 545 F.3d 1359, 1371 (Fed. Cir. 2008). In *Net MoneyIn*, the problem was that the district court found that a reference anticipated a claim to a five "link" Internet payment system only by combining "two separate disclosed examples." *Id.* at 1369. This Court reversed because the cited reference "disclose[d] two separate protocols for processing an Internet credit card transaction" but "[n]either of these protocols contain[ed] all five links arranged or combined in the same way as claimed." *Id.* at 1371.

Here, the Board did not physically combine separate embodiments to find that Beser anticipates. Rather, the Board agreed with the Examiner that the claimed "device" could be "an edge router, a communication device or both working in conjunction." Appx14. Thus, unlike the situation in *NetMoneyIN*, Beser's scheme in each of these various configurations functions the same way and is not rendered inoperative. Appx14.

The Board also relied on recognition in the '181 patent itself that functionality of a computer or networked system can be distributed across different devices or integrated into a single, physical device. Appx15 (citing Appx3351). The '181 patent explains, for example, that the "[s]ecure server computer 3320 can be a separate server computer from server computer 3304, or can be the same server computer having both non-VPN and VPN communication link capability, such as shown by server computer 3322." Appx113(51:15-29). What matters in the '181 patent is the *functionality* being performed, not what physical device houses that functionality. And in any event, recitation of "a first device" and "a second device" is nothing more than a "black box recitation of structure" for providing a specified function. *Williamson v. Citrix Online, LLC*, 792 F.3d 1339, 1350 (Fed. Cir. 2015) ("Generic terms such as … 'device,' and other nonce words that reflect nothing more than verbal constructs may be used in a claim in a manner that is tantamount to using the word 'means' … .").

Further, "*a* first device" does not mean that the first device can have only one element. The Board noted that this Court has "repeatedly emphasized that an indefinite article 'a' or 'an' in patent

parlance carries the meaning of 'one or more' in open-ended claims containing the transitional phrase 'comprising.'" Appx15 (quoting *KCJ Corp. v. Kinetic Concepts, Inc.*, 223 F.3d 1351, 1356 (Fed. Cir. 2000)). In fact, it is a "general rule[] of claim construction" that the "customary meaning of 'a'" is "one or more." *KCJ Corp.*, 223 F.3d at 1357. VirnetX's brief fails to even address—let alone attempt to distinguish—this basic doctrine of claim construction.

Notably, VirnetX also omits any discussion of this Court's recent decisions in *Kennametal, Inc. v. Ingersoll Cutting Tool Co.*, 780 F.3d 1376, 1381-83 (Fed. Cir. 2015) and *Blue Calypso, LLC v. Groupon, Inc.*, 815 F.3d 1331 (Fed. Cir. 2016), which rejected arguments similar to those VirnetX makes here. In *Kennametal*, the disputed claims were directed to a cutting tool assembled by a specific combination of materials, and the prior art reference disclosed a cutting tool assembled by combining different classes of materials with multiple options for each class, but the prior art reference did not explicitly disclose the specific combination recited in the claims. 780 F.3d at 1379-80. The Court affirmed the Board's anticipation finding, holding that "a reference can anticipate a claim even if it 'd[oes] not expressly spell out'

all the limitations arranged or combined as in the claim, if a person of skill in the art, reading the reference, would 'at once envisage' the claimed arrangement or combination." *Id.* at 1381 (citing *In re Petering*, 301 F.2d 676, 681 (1962)).

Similarly, in *Blue Calypso*, the patent owner argued that the Board "erroneously combined" two "separate and distinct" tools—the "targeted-marketing 'campaigns' tool and the refer-a-friend tool"—"to arrive at the claimed invention." 815 F.3d at 1342. The Court disagreed and found the Board's anticipation finding "distinguishable from *NetMoneyIN* because, in contrast to the reference in that case, [the reference at issue] explicitly contemplates the combination of the disclosed functionalities." *Id.* at 1343. The Court reiterated that "a reference need not always include an express discussion of the actual combination to anticipate," but rather that "a reference may still anticipate if that reference teaches that the disclosed components or functionalities may be combined and one of skill in the art would be able to implement the combination." *Id.* at 1344.

Although the Court also found it relevant that in *Blue Calypso* the Board had "reviewed expert testimony that supported its factual

determination that one of skill in the art would read the reference as disclosing the ability to combine the tools to arrive at the invention recited in the Blue Calypso Patents," 815 F.3d at 1343, the Court never suggested that expert testimony was *required* for the Board to make a factual conclusion about how one of skill in the art would read a reference. Here, the Board considered—and rejected—Dr. Keromytis' opinions because it was based on his erroneous understanding that the rejection required physically incorporating Beser's components. Appx14 (citing Appx2439).

2. Beser Discloses a "Secure Name" and "Unsecured Name"

VirnetX's argument that Beser does not disclose a "secure name" hinges on its (erroneous) claim construction. VirnetX Br. 42. Because the Board correctly construed "secure name" and "unsecured name," and VirnetX has not argued that Beser does not disclose these elements as defined by the construction adopted by the Board, VirnetX's argument should be rejected.

VirnetX argues that Beser does not show "resolution of the unique identifier into another network address by a secure name service." VirnetX Br. 42. But a "secure name" only needs to be "a name that

connotes a level of security," Appx10—a "secure name service" is not necessary. As the Board found, Beser's unique identifier connotes security. Appx16-17. First, the unique identifier is secure because it may be protected through encryption or authentication. Appx17; Appx604(11:22-25). Second, the unique identifier "create[s] and connote[s] a level of security" because it hides the identity of the network devices 24 and 26, thereby "ensuring anonymity." Appx17; Appx604(12:9-19).

3. Beser Discloses the Claimed "Receiving" and "Sending" Features

VirnetX argues that "Beser does not disclose [the] 'sending' and 'receiving' features," of claim 1 "because no single device alone performs these functions." VirnetX Br. 46. But, as the Board recognized, "claim 1 does not recite the message is received at any particular device or cannot be transmitted through an intermediary device." Appx19-20. And as explained before, VirnetX's argument that "[t]he Board's anticipation finding improperly groups multiple components or devices," VirnetX Br. 46, is contrary to this Court's precedent that "a reference may still anticipate if that reference teaches that the disclosed components or functionalities may be combined and one of skill in the

art would be able to implement the combination." *Blue Calypso*, 815 F.3d at 1344 (citing *Kennametal*, 780 F.3d at 1383).

VirnetX also argues that Beser does not disclose the "receiving" feature because Beser's request is received by the trusted-third-party network device rather than being received directly by the network devices 26 and/or 16. VirnetX Br. 48. But as the Board found, this argument ignores the breadth of claim 1, which "does not recite the message is received at any particular device or cannot be transmitted through an intermediary device." Appx19-20. Beser's step 106/116, which associates a public network address for a network device 16 through the trusted-third-party network device, meets the claimed receiving feature. Appx586-87(Fig. 5; Fig 6); Appx604(11:26-28). And even if claim 1 were to require that the message be received *at* the network device, Beser discloses that too, as the Board found. At Beser's step 108/118, "private IP addresses on network devices (e.g., 14 and 16) are negotiated using the public network and the private IP addresses are assigned to the terminating network devices (e.g., 24, 26)." Appx20 (citing Appx603(9:26-28, 9:46-49); Appx604(11:59-62; 11:67-12:4); Appx585-87(Figs. 4-6)). "That is, during negotiation between the

devices, messages are sent from one device (e.g., 14) and received at a network address corresponding to the secure name associated with another device (e.g., 16)." Appx20. VirnetX does not even address this finding. The Board correctly found that Beser discloses the claimed "receiving" and "sending" features.

4. Beser Discloses "Sending A Message Over A Secure Communication Link"

VirnetX's argument that Beser does not disclose "sending a message over a secure communication link" rests entirely on its incorrect construction of "secure communication link" as requiring encryption. VirnetX Br. 49. This argument fails for the reasons explained above.

Moreover, even if secure communication link requires encryption, *the Board found that Beser discloses encryption*. Appx17. VirnetX struggles to dismiss this finding in a footnote, characterizing it as relying on portions of Beser that discuss encryption of packets "*before* the tunnel is formed." VirnetX Br. 49 n.5. That is wrong on the facts and misrepresents Beser's disclosure.

Beser teaches that any IP packet that contains the unique identifier "may require encryption or authentication to ensure the

unique identifier cannot be read on the public network," Appx17 (citing Appx604(11:22-25)), and that such protection applies to IP packets sent after the tunnel is formed, Appx17 (citing Appx608(20:6-13), Appx609(22:8-22)). Beser then discloses that the public IP address for device 16 is used on a public network after the tunnel is formed in order to route packets to device 16 (by translating the private IP address for end device 26 into a routable address for device 16). Appx609(21:65-22:13; 22:44-48). However "secure communication link" is construed, Beser anticipates.

B. Substantial Evidence Supports the Board's Finding that Beser Anticipates Claims 2, 4, 9-11, and 24

VirnetX makes a variety of scattershot arguments challenging the Board's findings that Beser anticipates most of the remaining claims. But these underdeveloped arguments provide no basis for reversal.

1. Claim 2

VirnetX argues that "claim 2 also requires that the *same device* (i.e., the first device) *both* receive a message containing the network address associated with the secure name of the second device *and* send a message to the second device using the secure communication link." VirnetX Br. 49-50. VirnetX contends that the Board's anticipation

finding for claim 2 "rel[ied] on Beser's devices 14 and 24 working in tandem" and that the Board therefore made an "erroneous combination of multiple devices to anticipate the claimed 'same device' [sic]." VirnetX Br. 50. Yet again, VirnetX's argument is legally flawed because it simply fails to follow this Court's most relevant decisions. *See, e.g.*, *Blue Calypso*, 815 F.3d at 1343; *KCJ Corp.*, 223 F.3d at 1356-57.

2. Claim 4

Claim 4 recites that "the secure name indicates security." Appx115. The Board observed that this phrase is "quite broad" and concluded that Beser's unique identifier "indicates security" because it can be "a person's phone number, social security number, or domain name," which "are unique to [a] person," and because it "is used to create a secure communication link." Appx22.

VirnetX argues "a secure name in the '181 patent can indicate security, *for example*, through 'a non-standard top-level domain name, such as .scom' 'where the 's' stands for secure.'" VirnetX Br. 52 (emphasis added). But again, even VirnetX recognizes that these are non-limiting examples of how to "indicate security." Although VirnetX

faults the Board for concluding the phrase is "quite broad" purportedly without "making [any] attempt to construe the phrase in light of the specification or with evidence of how one of ordinary skill in the art would have understood the term," or purportedly "without any consideration of how the language in claim 4 might affect that conclusion," VirnetX 51-52, that criticism is curious at best since *neither does VirnetX*. Although VirnetX argues that "nothing about [Beser's] exemplary unique identifiers indicates or suggests security," VirnetX Br. 52, VirnetX never explains *why* the Board's factual finding on this point is erroneous, but rather only points to examples in the '181 patent. For example, VirnetX never explains why a phone number or social security number does not "indicate security" even though each is certainly not a "non-standard" domain name.

The Board correctly found that Beser's unique identifier "indicates security." The "unique identifier for a device provides security," Appx22, and Beser implements protocols such as encryption or authentication to hide it from discovery by untrusted parties. Appx604(11:13-25).

3. Claim 9

Claim 9 recites "automatically initiating the secure communication link after it is enabled." Appx115. The Board found that "Beser discloses the first and second network devices and the trusted-third-party network device negotiate addresses to create the tunnel for secure communications without involving an end user …, and thus the secure communication link is initiated automatically after the tunnel is enabled (e.g., after steps 116 and 118)." Appx22(citing Appx604(11:9-29, 11:59-62); Appx586-87(Fig. 5-6)).

VirnetX contends that "Beser does not address whether those steps involve a user, and therefore does not expressly disclose that they occur automatically." VirnetX Br. 53. But Beser explains that a trusted-third-party network device will negotiate with the first and second network devices to establish an IP tunnel between the first and second network devices. Appx602(7:62-63); Appx603(9:25-30). "The negotiation may occur through the trusted-third-party network device 30 to further ensure the anonymity of the telephone devices (24, 26)." Appx604(12:16-19). "Once negotiated," the private network IP addresses are used with the public IP addresses of the first and second

network devices to establish the tunnel automatically between the devices. Appx604(12:28-36); Appx2222-23.

In fact, Beser expressly discusses the ease to the user by automatically initiating the secure communication link. In describing the steps for initiating a VoIP association, Beser explains that "a user may simply be required to lift a telephone handset from its cradle and dial a conventional … telephone number," after which the trusted-third-party network device proceeds with the steps of initiating the secure communication link. Appx603(10:43-45); (Appx604(11:9-29; 11:59-62); Appx586-87(Fig. 5-6). Indeed, this is just as automatic as the '181 patent itself, which requires entering a domain name or selecting a hyperlink for initiating a secure communication link. Appx112(49:13-27).

VirnetX misplaces reliance on the unpublished decision *In re Giuffrida*, 527 F. App'x 981 (Fed. Cir. 2013). That case concerned claims to a "portable therapy system" for monitoring a patient's body motion and/or muscle activity, and the patent explained that "portable" meant that the device "is capable of being transported relatively easily." 527 F. App'x at 983-84. The Board found that a reference that disclosed

a device with a "rigid frame structure" and that could support a person's body nonetheless "inherently disclose[d] a portable system" because the reference did not have structure confining the device to a particular location. *Id.* at 985. The Court reversed the Board because the reference's silence on portability or lack thereof did not establish inherency, particularly in view of the proper construction of "portability" based on the patent's specification. *Id.* at 985-86.

Here, however, the Board did not rely on inherency. Rather, the Board found that Beser expressly disclosed this limitation. Appx22(citing Appx604(11:9-29, 11:59-62); Appx586-87(Figs 5-6).

Finally, VirnetX's argument that the Board purportedly failed to explain how Beser separately discloses both "enabling of the secure communication link" and "initiating" the link is wrong. VirnetX Br. 53. VirnetX does not contend now nor did it before the Board that "enabling" has any special meaning, and Beser describes the steps of "enabling" a secure communication link (Appx586-87(Figs 5-6)) that precede the link being initiated.

4. Claim 10 and 11

Claim 10 recites "wherein receiving a message containing the network address associated with the secure name of the device includes receiving the message at the first device through tunneling within the secure communication link." Appx115(56:9-13). Claim 11 recites "wherein receiving a message containing the network address associated with the secure name of the device includes receiving the message in the form of at least one tunneled packet." Appx115(56:14-17). VirnetX argues that "Beser does not disclose the features of either claim because Beser's tunneling association … is not set up at the time the alleged network address is received, and claims 10 and 11 require that the message containing that network address is received through the tunnel." VirnetX Br. 54. But VirnetX misreads Beser, which discloses that one of the security measures "is that of *initiating* and *maintaining* a virtual tunnel." Appx601(6:58-59)(emphasis added). In fact, Beser emphasizes the importance of protecting the negotiation process to protect the identities of the originating and terminating network devices. Appx604(12:6-19). And Beser further explains that

"[o]ne method" of protecting against hacking is by "initiating a tunneling connection" between network devices. Appx599(2:6-12).

5. Claim 24

Independent claim 24 recites the steps of "at the first device requesting and obtaining registration of a secure name for the first device" and "sending a message securely from the first device to the second device." Appx115. VirnetX contends that the Board erred by concluding "that Beser inherently discloses the claimed 'registration.'" VirnetX Br. 55. VirnetX theorizes that it is "possible" that, rather than requesting registration, Beser's unique identifier "might be pre-encoded into software on the trusted-third-party network device…." VirnetX Br. 55-56.

The problem for VirnetX is that these theoretical possibilities are contrary to Beser's disclosure. As the Board found, "Beser discloses the private IP addresses for the originating and terminating devices (e.g., 24 and 26) are recorded on the first and second network devices (e.g., 14 and 16) and addresses are stored in tables on these network devices." Appx23(citing Appx604(12:28-37)). Beser's device registration technique avoids problems where a user's IP addresses might change,

such as if a user switches offices or the IP addresses are dynamically assigned. Appx601(6:41-52); Appx603(10:55-11:2). Beser explains the trusted-third-party network device keeps track of registered devices by maintaining a database of subscribers, Appx604(11:45-58), which is the same registration technique disclosed in the '181 patent, Appx113(51:1-15). This is antithetical to a pre-encoded solution, and there is no basis for disturbing the Board's finding that Beser inherently discloses registration.

C. Substantial Evidence Supports the Board's Finding that Beser Anticipates Claims 3, 5-8, 12, 14, 15, 17-23, 25-29

VirnetX does not make any independent arguments for why Beser does not anticipate claims 3, 5-8, 12, 14, 15, 17-23, or 25-29, relying instead only on its arguments with respect to independent claims 1, 2, and 24. VirnetX Br. 57. Accordingly, because the Board correctly found that Beser anticipates claims 1, 2, and 24, the Court should affirm the Board's finding that Beser anticipates these claims too. *See Soverain Software LLC v. Newegg Inc.*, 728 F.3d 1332, 1335 (Fed. Cir. 2013) ("When a dependent claim and the independent claim it incorporates

are not separately argued, precedent guides that absent some effort at distinction, the claims rise or fall together").

III. THE COURT SHOULD AFFIRM THE BOARD'S FINDING THAT MATTAWAY ANTICIPATES CLAIMS 1, 2, 7-9, 12-17, 19-21, AND 24-29

A. Substantial Evidence Supports the Board's Findings that Mattaway Anticipates Claim 1

1. Mattaway Discloses a "Secure Name" and "Unsecured Name"

VirnetX makes two arguments for why Mattaway does not disclose the "secure name" and "unsecured name." VirnetX Br. 57-58. First, VirnetX argues that the Board erred by mapping "the claimed 'secure name' to the encrypted email address in Mattaway, and the 'unsecured name' to an alias," because VirnetX contends "the two names are functionally identical." VirnetX Br. 58. But this distorts Mattaway's disclosure. As the Board observed, Mattaway discloses that email addresses are located in a global server 1500 in a database 1516 that is located behind a firewall 1522, which protects against unauthorized access and prevents destruction of information. Appx25; Appx652(17:44-54: 18:19-40); Appx629-30(Figs. 15A-15B). The Board found that "[g]iven that these addresses are protected from destruction by the firewall, … these email addresses are made secure by the

firewall and connote a level of security." Appx25. On the other hand, the name or alias in Mattaway that the Board determined was an unsecured name is revealed when an incoming call arrives. Appx26; Appx656(26:45-47); *see also* Appx649(11:13-15). Mattaway's encrypted email address and Mattaway's alias are not the same, nor are they "functionally identical."

Second, VirnetX argues that Mattaway's email addresses that are hidden behind a firewall are not a "secure name" because, under VirnetX's proposed construction, a secure name must be "resolved by a secure name service." VirnetX Br. 58. Notably, VirnetX does not dispute that Mattaway's email address "connotes security" so as to be a secure name under the Board's construction. Rather, VirnetX's argument hinges on its erroneous circular claim construction requiring a secure name service.

VirnetX argues that "Mattaway does not have a secure name service that resolves secure names into network addresses" because "[t]he connection server 26 in Mattaway is a conventional name server of the type disclaimed by the '181 patent specification…." VirnetX Br. 58. But the Board correctly rejected VirnetX's disclaimer argument. As

the Board found, "the '181 patent does not disparage using a conventional scheme" or reject the conventional scheme as "transform[ing] the domain name into a secure name." Appx26. To the contrary, although the '181 patent indicates the conventional scheme suffers from drawbacks, the '181 patent nonetheless recognizes that it "'provides *secure* virtual private networks over the Internet.'" Appx26(citing Appx107(39:14-25). And as this Court has explained, "[a] patentee's discussion of the shortcomings of certain techniques is not a disavowal of the use of those techniques in a manner consistent with the claimed invention." *Epistar Corp. v. Int'l Trade Comm'n*, 566 F.3d 1321, 1335 (Fed. Cir. 2009).

2. Mattaway Discloses a "Message … of the Desire[] to Securely Communicate"

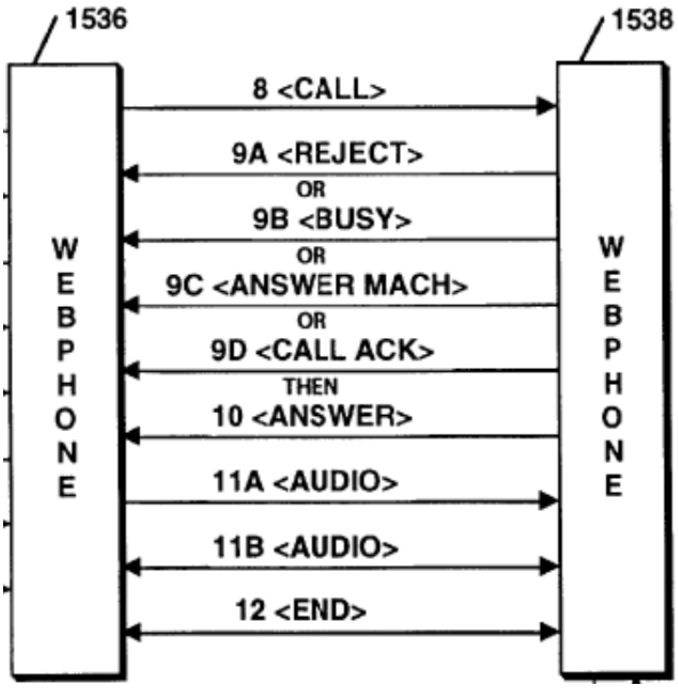
VirnetX's main dispute with the Board's finding that Mattaway discloses a "message … of the desire[] to securely communicate" is not that Mattaway fails to disclose it, but that the Board purportedly relied on a new grounds of rejection not adopted by the Examiner. VirnetX Br. 60-61. VirnetX states that the Examiner identified Mattaway's "<CONNECT> message" as the "message … of the desire[] to securely communicate" but that the Board identified instead the "<CALL>

packet" as that message. VirnetX Br. 60. But this misrepresents the prosecution history.

As the Board recognized, the Examiner in the Right of Appeal Notice (RAN) "adopted the rejection that includes mapping the <CALL> message" to the claimed "message." Appx27 (citing Appx2559-60 (RAN)). There, the Examiner found the <CONNECT> message, which is representative of the "'desire[] to securely communicate,' is received at the first device in the form of the <CALL> message." Appx2559. The Board's argument is the same argument upon which the Examiner relied, and VirnetX thus had "a fair opportunity to react to the thrust of the rejection." *See In re Jung*, 637 F.3d 1356, 1364-65 (Fed. Cir. 2011).

VirnetX also argues the rejection is wrong, suggesting the <CALL> message is "the call itself between the two devices," not the desire to securely communicate. VirnetX Br. 61-62. This is plainly not the case. If anything, the <CALL> message initiates a call wherein parties are able to communicate "in real-time, telephone quality, encrypted audio" over the internet. Appx656(25:31-34). This, by definition, expresses a "desire[] to securely communicate." Appx664(Claim 1). As illustrated in figure 17A (reproduced in relevant

part below), once the <CALL> packet is sent, a call is not necessarily initiated.



Appx634. Instead, "WebPhone 1538 may return with a number of different packets." Appx655(24:25-27). For example, it can be rejected with a <REJECT> packet, indicating "the callee WebPhone does not wish to be disturbed." Appx655(24:27-40). Similarly it can receive a <BUSY> packet indicating "the callee WebPhone is currently utilizing all available lines within its WebPhone application." Appx655(24:45-47). Communication is not initiated until an <ANSWER> packet is received. Appx656(25:13-46). At this point, parties send <AUDIO>

packets back and forth allowing for "real-time, telephone quality, encrypted audio communication over the Internet." Appx656(25:30-34).

B. Substantial Evidence Supports the Board's Findings That Mattaway Anticipates Claim 2, and Virnetx Has Waived Any Argument That Mattaway Does Not Disclose the Secure Name Service of Claim 2

VirnetX asserts that "the Board failed to even address whether Mattaway discloses the 'secure name service' explicitly recited in claim 2." VirnetX Br. 62. But before the Board, VirnetX *never* argued that Mattaway did not disclose a secure name service. Appx2291; Appx5036. VirnetX has thus waived this argument. *In re Baxter Int'l, Inc.*, 678 F.3d 1357, 1362 (Fed. Cir. 2012) ("Absent exceptional circumstances, … we generally do not consider arguments that the applicant failed to present to the Board.").

Even if VirnetX had not waived this argument, the Examiner found that Mattaway discloses the "secure name service" of claim 2, and VirnetX has not made any argument that the Examiner's finding is incorrect. Appx2202 (Action Closing Prosecution) (adopting the rejection proposed in the reexamination request); Appx194 (reexamination request) ("The connection server 26 acts as a secure name service … ."). Mattaway's connection server 26 is a secure name

service because it stores the network device address (e.g., the IP address of the callee) associated with the secure name of the callee's device, i.e., the callee's email address. Appx647(7:24-37).

C. Substantial Evidence Supports the Board's Findings That Mattaway Anticipates Claims 7-9, 12-17, 19-21, and 24-29

VirnetX makes no independent arguments with respect to claims 7-9, 12-17, 19-21, and 24-29. Therefore, these claims rise or fall with VirnetX's arguments with respect to claims 1 and 2. *See Soverain Software*, 728 F.3d at 1335.

IV. THE COURT SHOULD AFFIRM THE BOARD'S FINDINGS THAT PROVINO ANTICIPATES CLAIMS 1-15, 18-23, 28, AND 29

A. Substantial Evidence Supports the Board's Findings That Provino Anticipates Claim 1

1. Provino Discloses A First Device Associated with the "Secure Name" and "Unsecured Name"

Recycling the same arguments it makes as to Beser, VirnetX contends that the Board "mix[ed] and match[ed] devices" in finding that Provino disclosed the "first device." VirnetX Br. 64-65. But this misrepresents the Board's findings and ignores the broad scope of claim 1, which recites "a first device *associated with* a secure name and an unsecured name." Appx115. The Board found that "Provino discloses a

first device (e.g., server 31(s)) associated with a secure name as recited" because "servers 31(s) in Provino include human readable Internet addresses" that is "not accessible to servers (e.g., nameserver 17) and is located behind the firewall, which connotes a level [of] security for the name." Appx31. There is no error.

2. Provino Discloses a "Secure Name"

VirnetX argues that Provino does not disclose a "secure name" "because there is no name that requires resolution by a secure name service." VirnetX Br. 65. This argument, again, depends entirely on VirnetX's proposed erroneous construction of "secure name." VirnetX does not contest that the domain name for servers 31(s) "connotes a level of security," as required by the Board's construction of "secure name." Appx10; Appx31.

But even under VirnetX's construction, its argument fails. VirnetX contends that Provino's name server 32 "operate[s] in the conventional manner disclaimed in the '181 patent specification." VirnetX Br. 65. The Board rejected this same argument. Appx31-32. First, the Board "disagree[d] that the '181 patent has disclaimed a name server, such as server 32, from assisting in creating a secure

communication link as argued." Appx31. VirnetX's brief does not cite to any portion of the '181 patent for this supposed disclaimer. VirnetX's expert only identified a passage in the '181 patent that identified "certain drawbacks" in conventional schemes, Appx2012 (citing Appx107(39:23-25)), but identifying drawbacks does not equate to disclaimer. *See Epistar Corp. v. Int'l Trade Comm'n*, 566 F.3d 1321, 1335 (Fed. Cir. 2009) ("Disavowal requires 'expressions of manifest exclusion or restriction, representing a clear disavowal of claim scope.'").

Second, the Board found that even if such disclaimer existed, "server 32 in Provino, which is described as a 'VPN name server,' is not a standard DNS server on the public Internet and is located internal to VPN 15." Appx32. VirnetX does not dispute this finding, but instead argues that server 32 "operate[s] in the conventional manner." VirnetX Br. 65-66. But nothing in VirnetX's own proposed construction of "secure name" requires the "secure name service" to operate in a particular way—VirnetX did not even propose to the Board a construction for "secure name service." VirnetX's construction of "secure name" is impossibly circular, and the Board was correct in

rejecting it. Accordingly, the Board properly found that Provino discloses a secure name.

B. Substantial Evidence Supports the Board's Finding That Provino Anticipates the Remaining Claims

VirnetX makes no independent arguments with respect to claims 2-15, 18-23, 28, and 29, but rather merely refers back to its arguments with respect to claim 1. Accordingly, these claims rise or fall with VirnetX's argument with respect to claim 1. *See Soverain Software,* 728 F.3d at 1335.

CONCLUSION

For the foregoing reasons, the Board's final written decision should be affirmed.

May 26, 2016

Respectfully submitted,

/s/ John C. O'Quinn

John C. O'Quinn
Nathan S. Mammen
KIRKLAND & ELLIS LLP
655 15th Street, NW
Washington, DC 20005
(202) 879-5000

Jeffrey P. Kushan
SIDLEY AUSTIN LLP
1501 K Street, NW
Washington, DC 20005
(202) 736-8000

CERTIFICATE OF SERVICE

On May 26, 2016, the foregoing brief was submitted to the Court through the CM/ECF system. All participants in the case are represented by registered CM/ECF users and will be served electronically by the CM/ECF system.

/s/ Nathan S. Mammen

CERTIFICATE OF TYPE-VOLUME COMPLIANCE

This brief complies with the type-volume limitation specified in Federal Rule of Appellate Procedure 32(a)(7). According to the word processing system used to prepare this document, the brief contain 13,653 words.

/s/ Nathan S. Mammen